4. SIP Trunks

4.0.1 Background on SIP Trunks

The SIP Trunks are used for connecting PrivateServer to a local PBX or to a SIP VoIP provider. A Trunk can be used both for receiving and placing calls in a bidirectional way.

> ⚠ SIP trunks are mainly useful to interconnect EVSS ecosystem with other SIP infrastructure, using an end-to-site security model, featured by **PrivateWave Enterprise Edition**. SIP trunks have a very limited usefulness for **PrivateWave Professional Edition**.

Each SIP Trunk can be used to both receive and place calls.

4.0.2 SIP Trunk's categories

From the PrivateServer version 2.5 you have two main SIP Trunk's categories:

1. **Secure** Trunks
2. **Insecure** Trunks

The former ones entail both **TLS and SRTP**, while the latter none of them: they use just **RTP over UDP** (thus **without TLS**). Which one is to be used depends on many factors, major one is the kind of PBX on the trunk's end. For example **Cisco Unified Communications Manager** are usually connected to PrivateServer via **Secure Trunk**, while SIP providers most often use the **Unsecure Trunk**.

4.0.3 Authentication Models in SIP Trunks

Apart for trunk's categories, you should get acquainted with the Authentication Model, that can be:

1. **SIP Account** for Registered Trunks
2. **IP Authenticated** for Unregistered Trunks

SIP Trunks using the Registered Authentication Model need an account on the other end. Then they use the account's credential to authenticate the Trunk when the PrivateServer is started and every communication that passes over that Trunk is considered authenticated, thus valid by default, and has the right to be processed and routed.

SIP Trunks with no registration, on the other hand, do not need for an account to be setup: instead they use IP address to authorize every SIP communication directed to the PrivateServer . This model implies that any new SIP communication is authenticated against the sender's IP address (meaning the one belonging to the PBX connected to the PrivateServer).

The latter model is mostly used enterprise systems, eg with CUCM. The former is mostly used with SIP Providers.

> ⊘ There's no way to perform an unauthenticated SIP INVITE on PrivateServer ! You can have different authentication models but you cannot choose to enable an unauthenticated SIP Trunk.

4.0.4 General starting point for SIP Trunk configuration

No matter what kind of Trunk you're going to configure on PrivateServer , you would anyway come throughout the SIP Trunk configuration page in order to complete your setup.

figure 1. New SIP Trunk form

in figure 1. New SIP Trunk form it's shown the tipical generic new sip trunk form.

The fields have the following meanings:

- **NAME:** a meaningful name for this trunk
- **FAILOVER GROUP:** choose if this trunk belongs to a failover group
- **IP / HOSTNAME**: IP address or Hostname of the SIP server provided by ITSP
- **PORT**: registration port of the service
- **TRANSPORT**: protocol to be used as a transport mean. Choices are:
  - **UDP**
  - **TLS**
- **OUTBOUND PROXY**: IP address of the outbound proxy server provided by ITSP
- **REGISTER**: select if you want to have only outgoing calls or incoming (see below for deeper explanation)
- **USERNAME**: login username
- **PASSWORD**: password for the username entered above
- **VIRTUAL PHONE NUMBER**: associated virtual number
- **SIP OPTIONS PING**: select it if you want PrivateServer to send a SIP OPTIONS packet on a regular basis

- **ENABLE SIP URIs:**
  - **NO**
  - **YES**
  - **AUTOMATIC**
- **SRTP ENCRYPTION**: whether the trunk has to be encrypted or not
- **SRTP CRYPTO SUITE:** which type of crypto to be used for SRTP communication
  - **AES128**
  - **AES256**
- **SECURE RTCP:**
  - **AUTHENTICATED**
  - **ENCRYPTED**
  - **AUTHENTICATED AND ENCRYPTED**
- **INSECURE CALL TREATMENT:** if SRTP ENCRYPTION is selected and call goes to an insecure route choose one of the above options
  - **ACCEPT**
  - **REJECT**
  - **REJECT WITH ANNOUNCEMENT**
- **MAX CONCURRENT CALLS**: maximum number of calls on a single trunk
- **NAT**: enable/disable the Network Address Translation configuration
- **DIRECTMEDIA**: experimental sound management in P2P mode without routing the audio stream through the server
- **SEND REMOTE-PARTY-ID**: the Remote Party ID, used to interconnect with VoIP Provider for the management of privacy
- **CODECS:** voice codecs used in this trunk
- **ANNOUNCEMENT**: this is used for Audio Messaging. The possible values are:
  - **NO**: no audio messages would be played on this trunk
  - **ON EARLY MEDIA**: the audio messages would be played using SIP early media
  - **ON ANSWERED CALLS**: the audio messages would be played after answering the call
- **DTMF SIGNALING METHOD**
- **Trusted**: audio disclaimer is played if the trunk is not trusted

figure 2. SIP Trunk section in call routing menu

You can reach figure 1. New SIP Trunk form using the **CALL ROUTING** menu inside the Configuration. As you can read in figure 2. SIP Trunk section in call routing menu there are just 2 links inside it:

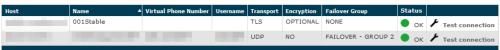- **SIP Trunks**
- **Outbound**

figure 3. The SIP Trunk list

For creating a new SIP Trunk you go on the **SIP Trunks** menu voice and then use the **New SIP Trunk** in the **SIP Trunk List** page (see figure 3. The SIP Trunk list.

For each category and authentication models you are going to find a specific manual page describing the correct configuration and the possible parameters to be used.

4.1 ENCRYPTED SIP Trunks